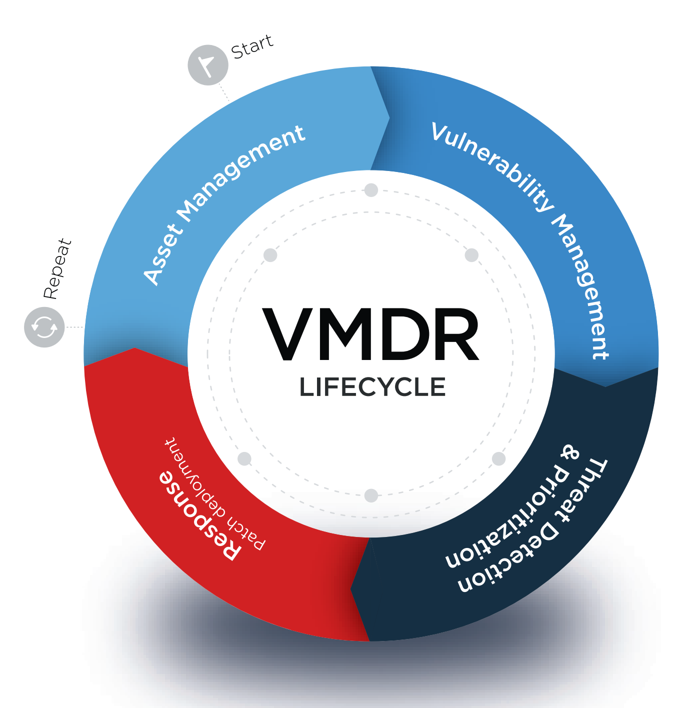


Qualys VMDR® — Une solution tout-en-un pour la gestion, la détection et la réponse aux vulnérabilités

La principale solution de gestion des vulnérabilités du marché atteint de nouveaux sommets

Découvrez, évaluez, hiérarchisez et corrigez les vulnérabilités critiques en temps réel et à travers votre paysage IT hybride et mondial, le tout via une solution unique.



VMDR avec orchestration intégrée



Identifiez tous les actifs connus et inconnus au sein de votre environnement informatique hybride global

Pour des raisons de sécurité, il est vital de savoir ce qui est actif dans un environnement IT hybride mondialisé. Détectez automatiquement tous les actifs connus et inconnus partout où ils se trouvent pour disposer d'un inventaire complet, classé, riche en détails, notamment sur le cycle de vie fournisseur et bien d'autres éléments encore.



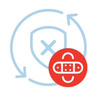
Analysez les vulnérabilités et les problèmes de configuration avec une précision d'analyse Six Sigma

Détectez automatiquement les vulnérabilités et les problèmes de configuration critiques d'après les bancs d'essai du Centre pour la Sécurité sur Internet (CIS).



Concentrez-vous rapidement sur le plus urgent

À l'aide d'une fonction de corrélation de pointe et d'apprentissage automatique, hiérarchisez automatiquement les vulnérabilités les plus risquées pour vos actifs les plus critiques et passez ainsi de plusieurs milliers à quelques centaines de vulnérabilités importantes.



Inoculez vos actifs contre les menaces les plus graves

Déployez en un seul clic le patch le plus pertinent pour remédier rapidement les vulnérabilités et les menaces dans les environnements de toute taille.

Aujourd'hui, les processus impliquent différentes équipes et s'appuient sur de nombreuses solutions spécifiques, ce qui rend le déploiement de patches critiques encore plus complexe et long.

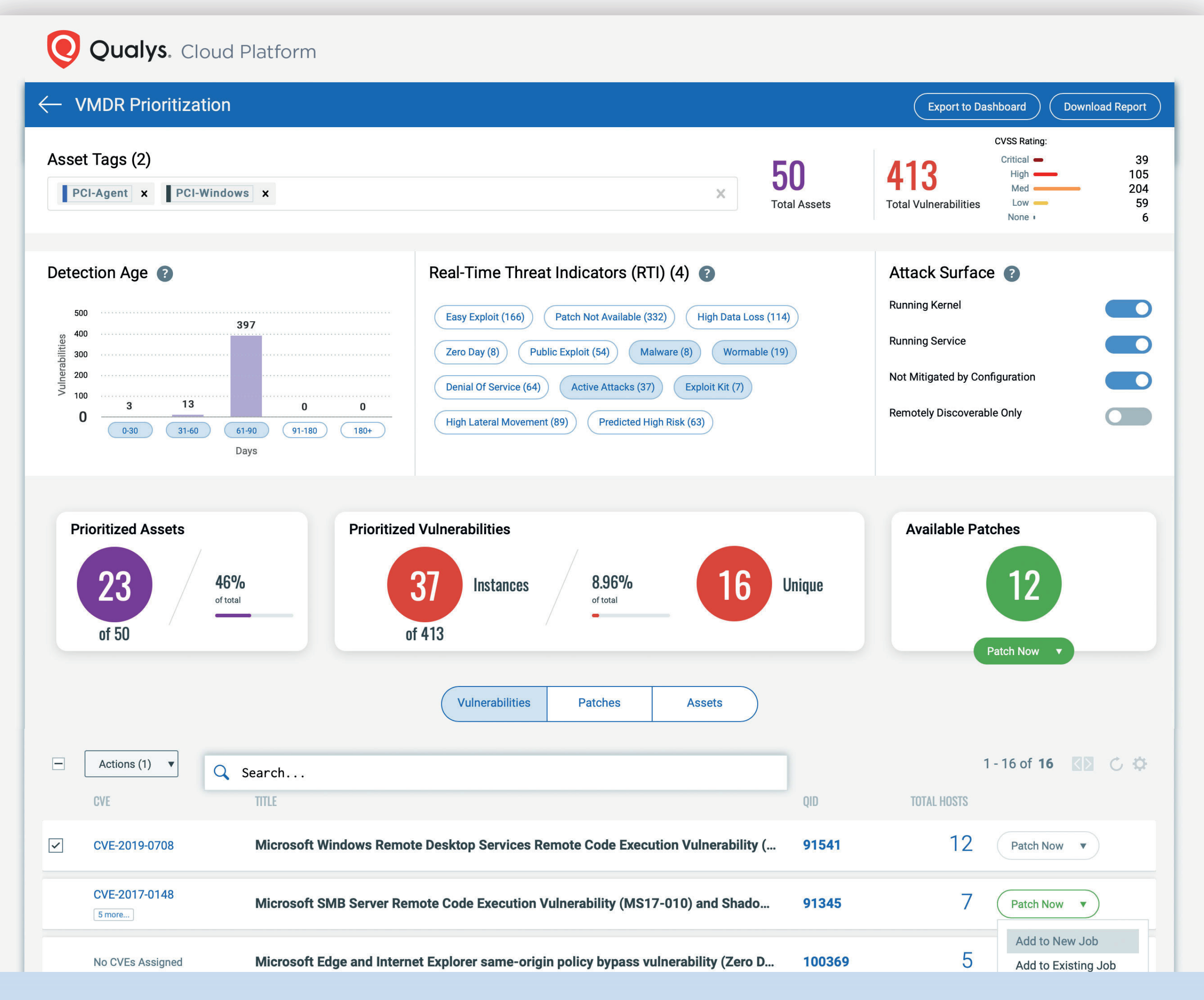
Les solutions spécifiques traditionnelles ne s'interfaçent pas très bien entre elles et sont donc une source de problèmes d'intégration, de faux positifs et de retard. De même, les équipements ne sont pas identifiés, les actifs critiques sont mal classés, les vulnérabilités sont hiérarchisées de manière incorrecte et les patches ne sont pas pleinement déployés.

Une application unique pour la découverte, l'évaluation, la détection et la réponse

Les agents Cloud légers mais puissants, les scanners virtuels, les ressources d'analyse (passive) du réseau et Qualys Cloud Platform sont les quatre éléments-clés d'un programme de gestion des vulnérabilités performant réunis au sein d'une application unique et unifiée par de puissants workflows d'orchestration prêts à l'emploi. Grâce à Qualys VMDR®, les entreprises peuvent découvrir automatiquement chaque actif présent dans leur environnement, y compris ceux non administrés qui apparaissent sur le réseau, et également inventorier tous les matériels et logiciels et classer et marquer les actifs critiques. VMDR recherche en permanence les toutes dernières vulnérabilités sur ces actifs en s'appuyant sur les informations sur les menaces les plus récentes pour hiérarchiser activement la remédiation des vulnérabilités exploitables. Enfin, VMDR détecte automatiquement les tout derniers patches les plus pertinents pour les actifs vulnérables et les déploie facilement à des fins de remédiation.

Orchestration intégrée

En fournissant toutes ces fonctionnalités via un workflow intégré à une application unique, VMDR automatise l'ensemble du processus et accélère sensiblement la capacité de l'entreprise à répondre aux menaces et à éviter leur exploitation.



Avantages majeurs



Tout est dans le Cloud

Pas besoin d'appliances volumineuses. Tout est dans le Cloud et prêt à fonctionner.



Déploiement aisé

Le déploiement est d'une simplicité incroyable. Grâce à des scanners virtuels illimités, vous pouvez activer un scanner et l'utiliser en un rien de temps.



VM comprise

VMDR offre la même solution de gestion des vulnérabilités que celle à laquelle vous êtes habitués et faites confiance, ainsi que de nombreuses autres applis extraordinaires.



Réduction sensible des délais et des coûts

En s'appuyant sur une plateforme Cloud unique, les entreprises font des économies substantielles au niveau des ressources et du temps nécessaires à l'installation de nombreux agents et de multiples consoles et intégrations.



GESTION DES ACTIFS

Identification et catégorisation automatisées des actifs

Pour des raisons de sécurité, il est vital de savoir ce qui est actif dans un environnement IT hybride mondialisé. Grâce à Qualys VMDR, les entreprises peuvent découvrir et classer automatiquement leurs actifs connus et inconnus, identifier en permanence les actifs non administrés et créer des workflows automatisés pour les gérer efficacement.

Une fois les données collectées, il est possible d'interroger instantanément les actifs et un quelconque attribut pour une meilleure visibilité notamment sur les matériels, la configuration système, les applications, les services et les connexions réseau.



GESTION DES VULNÉRABILITÉS

Une détection en temps réel des vulnérabilités et des problèmes de configuration

Grâce à VMDR, détectez automatiquement les vulnérabilités et les problèmes de configuration critiques sur chaque actif en vous référant aux bancs d'essai du Centre pour la Sécurité sur Internet (CIS). Les problèmes de configuration entraînent des violations et des défauts de conformité, ce qui crée des vulnérabilités sur des actifs non affectés par des vulnérabilités et des expositions courantes (CVE). La solution VMDR identifie en permanence les vulnérabilités critiques et les problèmes de configuration sur le plus large éventail d'équipements, de systèmes d'exploitation et d'applications disponibles sur le marché.



HIÉRARCHISATION DES MENACES

Hiérarchisation automatisée de la remédiation

Qualys VMDR s'appuie sur les informations disponibles en temps réel sur les menaces et sur des modèles d'apprentissage automatique pour automatiser la hiérarchisation des vulnérabilités les plus dangereuses présentes sur les actifs les plus critiques. Des indicateurs d'exploitabilité, d'attaque active ou de mouvement latéral d'envergure signalent les vulnérabilités qui présentent des risques tandis que des modèles d'apprentissage automatique identifient les vulnérabilités les plus susceptibles de se transformer en menaces graves, ce qui garantit donc plusieurs niveaux de hiérarchisation.



GESTION DES PATCHES

Correctifs et remédiation à portée de clavier

Après avoir hiérarchisé les vulnérabilités selon leur niveau de risque, la plateforme VMDR procède rapidement à la remédiation ciblée des vulnérabilités dans des environnements de toute taille en déployant le correctif le plus pertinent. En outre, des tâches récurrentes, automatisées et fondées sur des politiques maintiennent les systèmes à jour, ce qui garantit une gestion proactive des patches ayant ou non un rapport avec la sécurité. Ceci permet de réduire sensiblement le nombre de vulnérabilités que l'équipe d'exploitation doit traquer dans le cadre du cycle de remédiation.



Confirmation et répétition

En outre, VMDR complète le cycle de vie de gestion des vulnérabilités à partir d'une vue unifiée fournie par des tableaux de bord et des assistants personnalisables en temps réel qui intègrent une analyse des tendances. Reposant sur un modèle tarifaire par actif et sans logiciel à mettre à jour, VMDR réduit sensiblement votre coût total de possession.

Qualys VMDR® — Vérifiez par vous-même.

Applis et services	Intérêt	*Inclus*	*Complémentaire*
GESTION DES ACTIFS			
Asset Discovery	Détectez et inventoriez tous les actifs connus et inconnus qui se connectent à votre environnement informatique hybride global, qu'il s'agisse d'équipements et d'applications sur site, de terminaux mobiles, de points d'extrémité, de clouds, de conteneurs ou d'OT/IoT. Capteurs Qualys Passive Scanning Sensor inclus.	○	
Asset Inventory Disposez d'un inventaire en temps réel et actualisé de tous les actifs IT.	• **Inventaire des équipements sur site** – Détectez tous les équipements et toutes les applications connectés au réseau (serveurs, bases de données, postes de travail, routeurs, imprimantes, équipements IoT, etc.). • **Inventaire des certificats** – Détectez et classez tous les certificats numériques TLS/SSL (internes et externes) émis par une autorité de certification. • **Inventaire Cloud** – Surveillez les utilisateurs, les instances, les réseaux, le stockage, les bases de données et leurs relations pour avoir un inventaire permanent des ressources et des actifs sur toutes les plateformes Cloud publiques. • **Inventaire des conteneurs** – Découvrez et suivez l'infrastructure des conteneurs dans tous les environnements. • **Inventaire des équipements mobiles** – Détectez et classez chaque équipement mobile de l'entreprise grâce à des informations complètes sur l'équipement, sa configuration et les applications installées dessus.	○	
Classification et normalisation des actifs	Collectez des informations détaillées, notamment sur l'actif, les services exécutés et les logiciels installés. Supprimez les différents noms des produits et des fournisseurs et classez les actifs par gammes de produits.	○	
Informations enrichies sur les actifs	Obtenez des détails approfondis et inédits, notamment sur les cycles de vie matériels/logiciels (EOL/EOS) et un audit des licences logicielles et des licences commerciales et Open Source.		○
CMDB Synchronization	Synchronisez les informations sur les actifs de manière bidirectionnelle entre Qualys et le système de gestion des configurations CMDB ServiceNow.		○
GESTION DES VULNÉRABILITÉS			
Vulnerability Management	Détectez en continu les vulnérabilités logicielles grâce à la base de données de signatures la plus complète sur le plus large éventail de catégories d'actifs. Qualys est le leader du marché de la gestion des vulnérabilités.	○	
Configuration Assessment	Évaluez, signalez et surveillez les problèmes de configuration liés à la sécurité d'après les bancs d'essai de sécurité du Centre pour la Sécurité sur Internet (CIS).	○	
Certificate Assessment	Évaluez vos certificats numériques (internes et externes) et vos configurations TLS pour détecter les problèmes de certificat et les vulnérabilités.		
Modules d'évaluation supplémentaires	• **Évaluation de la sécurité Cloud** – Supervisez et évaluez en permanence vos ressources PaaS/IaaS pour y détecter des erreurs de configuration et des déploiements non conformes. • **Évaluation de la sécurité des conteneurs** – Analysez les images des conteneurs et les conteneurs exécutés présents dans votre environnement pour y rechercher des vulnérabilités particulièrement sérieuses et des logiciels non approuvés avant de lancer des opérations de remédiation. Des modules supplémentaires pour les outils CI/CD et les registres permettent aussi d'analyser la phase de développement (build).		○
DÉTECTION ET HIÉRARCHISATION DES MENACES			
Continuous Monitoring	Soyez avertis en temps réel des anomalies réseau. Ce service identifie les menaces et surveille les changements non planifiés sur votre réseau avant qu'ils ne se transforment en failles.	○	
Threat Protection	Identifiez les menaces les plus critiques et hiérarchisez le déploiement des correctifs. Avec des informations en temps réel sur les menaces et l'apprentissage automatique, contrôlez les menaces qui évoluent sans cesse et identifiez celles à remédier en priorité.	○	
RÉPONSE			
Patch Detection	Corrélez automatiquement les vulnérabilités et les correctifs pour des serveurs spécifiques et accélérez ainsi la remédiation. Recherchez les vulnérabilités et expositions courantes (CVE) et identifiez les correctifs les plus récents et appropriés.	○	
Patch Management via Third-Party Vendors	Intégration à vos solutions de déploiement de patches existantes, notamment SCCM et autres solutions tierces pour accélérer sensiblement le déploiement des correctifs.		○
Patch Management via Qualys Cloud Agents	Utilisez les agents Cloud Qualys pour accélérer le déploiement des patches sans dépendre de solutions de déploiement de correctifs tierces.		○
Container Runtime Protection	Sécurisez, protégez et supervisez les conteneurs exécutés dans des environnements traditionnels de conteneurs sur des serveurs et dans des environnements de conteneurs en tant que service en appliquant des politiques comportementales granulaires. (Disponible T2/T3 2020)		○
Mobile Device Management	Supervisez, gérez et sécurisez à distance vos équipements mobiles. (Disponible en version bêta au 2ème trimestre 2020)		○
Renouvellement des certificats	Renouvelez les certificats arrivés à expiration directement via Qualys (option disponible au 2ème trimestre 2020)		
Offre VMDR en version ILLIMITÉE : Qualys Virtual Passive Scanning Sensors (pour la découverte), Qualys Virtual Scanners, Qualys Cloud Agents, Qualys Container Sensors et Qualys Virtual Cloud Agent Gateway Sensors pour optimiser la bande passante.		○	